

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-281013

(43)Date of publication of application : 27.09.2002

(51)Int.Cl.

H04L 9/08

G06F 12/14

H04L 9/10

(21)Application number : 2001-382149

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 14.12.2001

(72)Inventor : NAKANO TOSHIHISA
MATSUZAKI NATSUME
TATEBAYASHI MAKOTO

(30)Priority

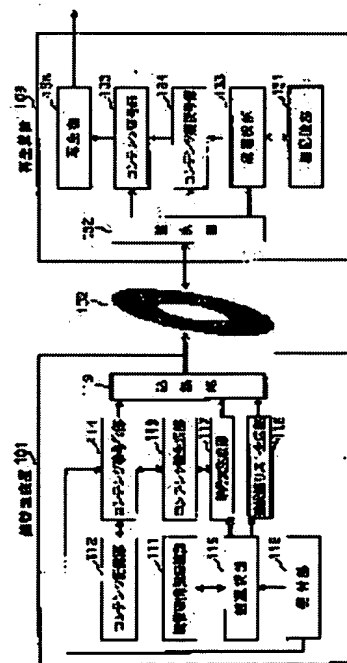
Priority number : 2000384389 Priority date : 18.12.2000 Priority country : JP

(54) KEY MANAGEMENT DEVICE FOR PROTECTING COPYRIGHT, RECORDING MEDIUM, REPRODUCTION DEVICE, RECORDING DEVICE, KEY MANAGEMENT METHOD, REPRODUCTION METHOD, KEY MANAGEMENT PROGRAM, AND COMPUTER READABLE RECORDING MEDIUM WITH KEY MANAGEMENT PROGRAM RECORDED

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a key management device capable of managing a key assigned to a reproduction device.

SOLUTION: The key groups of keys arranged in each node in a tree structure having N layers on different paths following those keys from the Nth layer to the uppermost layer are respectively assigned to different reproduction devices. In receiving the notification of the key group of one reproduction device, a key selecting part 115 defines the respective keys of the key group as an invalid key, and selects a key in the further lower layer of the invalid key which is assigned to another reproduction device, and which is not defined as the invalid key on another path as a selection key. A contents enciphering part 114 generates data by enciphering the contents with a contents key. A cipher text generating part 117 generates a cipher text by enciphering the contents key with the selected selection key. A selection key list generating part 118 generates the list of the selection keys used for the generation of the cipher text. A recording part 119 records the data and the cipher text and the list in a recording medium.



LEGAL STATUS

[Date of request for examination]

12.10.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the
examiner's decision of rejection or application
converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration] ·

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-281013

(P2002-281013A)

(43)公開日 平成14年9月27日(2002.9.27)

(51)Int.Cl. ⁷	識別記号	F I	テーマコード*(参考)
H 0 4 L 9/08		G 0 6 F 12/14	3 1 0 K 5 B 0 1 7
G 0 6 F 12/14	3 1 0		3 2 0 B 5 J 1 0 4
	3 2 0	H 0 4 L 9/00	6 0 1 Z
H 0 4 L 9/10			6 2 1 A

審査請求 未請求 請求項の数22 O L (全 21 頁)

(21)出願番号 特願2001-382149(P2001-382149)
(22)出願日 平成13年12月14日(2001.12.14)
(31)優先権主張番号 特願2000-384389(P2000-384389)
(32)優先日 平成12年12月18日(2000.12.18)
(33)優先権主張国 日本(J P)

(71)出願人 000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者 中野 稔久
大阪府門真市大字門真1006番地 松下電器
産業株式会社内
(72)発明者 松崎 なつめ
大阪府門真市大字門真1006番地 松下電器
産業株式会社内
(74)代理人 100090446
弁理士 中島 司朗

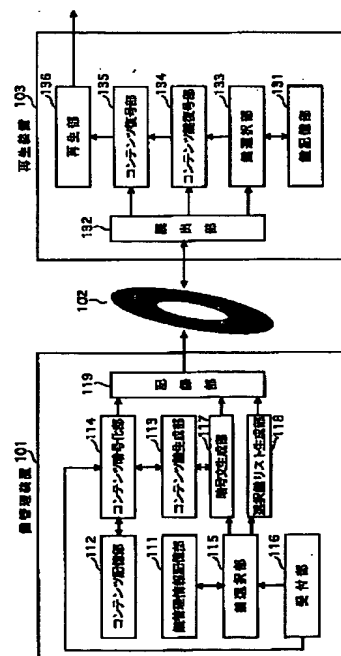
最終頁に続く

(54)【発明の名称】 著作権保護のための鍵管理装置、記録媒体、再生装置、記録装置、鍵管理方法、再生方法、鍵管理プログラム及び鍵管理プログラムを記録したコンピュータ読み取り可能な記録媒体

(57)【要約】

【課題】 再生装置に割り当てた鍵を管理する鍵管理装置を提供する。

【解決手段】 N層の木構造の各ノードに配置された鍵の第N層から最上層の鍵に辿る異なる経路上の鍵群は、それぞれ異なる再生装置に割り当てられている。鍵選択部115は、1つの再生装置が有する鍵群の通知を受けると、当該鍵群の各鍵を無効鍵とする。無効鍵の一層下層の他の再生装置に割り当てられた他の経路上の鍵で無効鍵でない鍵を選択鍵として選択する。コンテンツ暗号化部114はコンテンツをコンテンツ鍵で暗号化したデータを生成する。暗号文生成部117は、コンテンツ鍵を選択した選択鍵で暗号化した暗号文を生成する。選択鍵リスト生成部118は、暗号文の生成に用いた選択鍵のリストを生成する。記録部119は、データと暗号文とリストとを記録媒体に記録する。



【特許請求の範囲】

【請求項1】 暗号化されたデータを復号して再生する複数の再生装置に割り当てた鍵を管理する鍵管理装置であって、

木構造は少なくとも1つあり、木構造の第N層の鍵から最上層の鍵に辿る異なる経路上の鍵群は、それぞれ異なる再生装置に割り当てられているN（Nは、2以上の自然数）層の木構造の各ノードに配置された鍵を記憶している鍵記憶手段と、

前記各鍵群のうち、1つの再生装置が有する鍵群の情報の通知を受けると、当該鍵群の各鍵を無効鍵とし、無効鍵を経路上のノードに持つ他の再生装置に割り当てられた鍵群のうちから、前記無効鍵より一層下層の無効鍵でない鍵を選択し、前記データの暗号化に用いたコンテンツ鍵を当該選択した鍵で暗号化した暗号文と、当該選択した鍵を特定する特定情報とからなる暗号情報を生成する暗号情報生成手段とを備え、

前記各再生装置は、割り当てられたN個の鍵を記憶しており、前記特定情報により特定される鍵を用いて対応する暗号文を復号してコンテンツ鍵を得、前記データをそのコンテンツ鍵で復号して、コンテンツを再生することを特徴とする鍵管理装置。

【請求項2】 前記暗号情報生成手段は、コンテンツをコンテンツ鍵で暗号化したデータを生成するデータ生成部と、

1つの再生装置に割り当てられた鍵群の情報の通知を受け付ける無効鍵受付部と、

通知された鍵群に含まれる各鍵を無効鍵とし、無効鍵の第N層を除く一層下層の異なる経路上の無効鍵でない鍵を選択鍵として選択する鍵選択部と、

前記コンテンツ鍵を前記各選択鍵で暗号化した暗号文を生成する暗号文生成部と、

前記各選択鍵を識別するリストを生成する選択鍵リスト生成部とを有することを特徴とする請求項1記載の鍵管理装置。

【請求項3】 前記鍵管理装置の鍵記憶手段は、各鍵ごとに、その鍵を識別する識別子と、その鍵の経路上の一層上層の親鍵を識別する識別子と、その鍵が前記暗号文の生成に用いられている選択鍵か、無効鍵か、そのいずれでもない未使用鍵かの状態を示す鍵状態情報と、鍵データとを記載した鍵管理情報を記憶している鍵管理情報記憶部を有し、

前記無効鍵受付部は、鍵群の各鍵の識別子を知り、前記鍵選択部は、前記鍵管理情報の各鍵の識別子と通知された識別子とが、一致するとき前記鍵状態情報を無効鍵に更新し、一致しないとき親鍵が無効鍵であって自身が無効鍵でも選択鍵でもない未使用鍵のとき前記鍵状態情報を選択鍵に更新することを特徴とする請求項2記載の鍵管理装置。

【請求項4】 前記鍵管理情報において、最上層の鍵の

親鍵を識別する識別子には、特定の値が記載され、前記鍵選択部は、識別子に特定の値が記載された鍵の鍵情報が無効鍵でないときに選択鍵とすることを特徴とする請求項3記載の鍵管理装置。

【請求項5】 前記暗号情報生成手段は、一旦無効鍵とした鍵で復号させるべき1つの再生装置が有する鍵群の情報の通知を受け付ける復号鍵受付手段と、

通知された鍵群に含まれる鍵の経路上の一層上層の親鍵が無効鍵であり、その親鍵を共通の親鍵とする異なる経路上の鍵が共に無効鍵であるとき、その通知された鍵群に含まれる鍵を選択鍵とし、その選択鍵より下層の同一の経路上の鍵群の各鍵を選択鍵でも無効鍵でもない未使用鍵とする鍵復号部とを更に有することを特徴とする請求項2記載の鍵管理装置。

【請求項6】 前記鍵記憶手段は、各鍵ごとに、その鍵を識別する識別子と、その鍵の経路上の一層上層の親鍵を識別する識別子と、その鍵が前記暗号文の生成に用いられている選択鍵か、無効鍵か、そのいずれでもない未使用鍵かの状態を示す鍵状態情報と、鍵データとを記載した鍵管理情報を記憶している鍵管理情報記憶部を有し、

前記復号鍵受付部は、鍵群の各鍵の識別子を知り、前記鍵復号部は、前記鍵管理情報の各鍵の識別子と通知された識別子とが一致する場合、当該鍵が最上層の鍵であるとき、一層下層の異なる経路上の鍵が選択鍵であるとき、鍵状態情報を選択鍵に更新し、当該鍵が最上層の鍵以外であるとき、当該鍵の親鍵を共通にする異なる経路上の鍵が共に無効鍵であるとき、当該鍵の鍵状態情報を選択鍵に更新し、その選択鍵より下層の同一経路上の通知された識別子を有する各鍵の鍵状態情報を無効鍵、選択鍵のいずれでもない未使用鍵に更新し、通知された識別子と一致しない場合、その親鍵の鍵状態情報を選択鍵に更新したとき、鍵状態情報を未使用鍵に更新することを特徴とする請求項5記載の鍵管理装置。

【請求項7】 前記鍵管理装置は、新たに鍵群を割り当てる再生装置数を受け付ける新規受付手段と、

木構造の第M層の鍵数を、再生装置数以上とするM（Mは2以上N以下の自然数）層の木構造の各ノードに配置された鍵を生成する新規鍵生成手段と、前記新規鍵生成手段で生成された木構造の最上層の鍵を既に鍵記憶手段に記憶されている（N-M+1）層以上の選択鍵又は未使用鍵に変更する接続手段とを更に備えることを特徴とする請求項2記載の鍵管理装置。

【請求項8】 前記鍵管理装置は、前記データ生成部で生成されたデータと、前記暗号文生成部で生成された暗号文と、前記選択鍵リスト生成部で生成されたリストとを記録媒体に記録する記録手段を更に備えることを特徴とする請求項2記載の鍵管理装置。

【請求項9】 前記鍵管理装置は、前記データ生成部で生成されたデータと、前記暗号文生成部で生成された暗号文と、前記選択鍵リスト生成部で生成されたリストとを複数の再生装置に送出する送出手段を更に備えることを特徴とする請求項2記載の鍵管理装置。

【請求項10】 前記鍵管理情報記憶部は、前記鍵選択部により更新される鍵管理情報を記憶しておき、前記鍵記憶手段は、初期状態又はいずれかの更新時の状態に鍵管理情報を復帰させる復帰部を有することを特徴とする請求項3記載の鍵管理装置。

【請求項11】 前記無効とする鍵群の数の最大値を2Kとすると、前記鍵記憶手段に記憶されている木構造の数Lは $2K+1$ とすることを特徴とする請求項1記載の鍵管理装置。

【請求項12】 N（Nは、2以上の自然数）層の木構造の各ノードに配置された鍵の第N層の鍵から最上層の鍵に辿る異なる経路上の1つの鍵群を記憶している再生装置で再生される記録媒体であって、コンテンツをコンテンツ鍵で暗号化したデータを記憶しているデータ領域と、前記コンテンツ鍵を暗号化した少なくとも1つ以上の暗号文を記憶している暗号文領域と、前記暗号化に用いた鍵を識別する情報が記憶されている選択鍵リスト領域とを有し、暗号化に用いた選択鍵は、特定の再生装置以外の他の再生装置に記憶されている鍵群に含まれる1つの鍵と一致していることを特徴とする記録媒体。

【請求項13】 暗号化したデータを復号して再生する再生装置であって、各鍵は、N（Nは、2以上の自然数）層の木構造の各ノードに配置された鍵の木構造の第N層の鍵から最上層の鍵に辿る異なる経路上の1つの経路上にある鍵であるN個の鍵を記憶している鍵群記憶手段と、コンテンツをコンテンツ鍵で暗号化したデータと、前記コンテンツ鍵を暗号化した暗号文と、暗号化に用いた鍵を識別する情報とを取得する、暗号文は少なくとも1つ以上ある再生情報取得手段と、前記鍵を識別する情報で識別される鍵を前記鍵群記憶手段に記憶されている鍵から選択し、当該選択した鍵に対応する暗号文を復号してコンテンツ鍵を得るコンテンツ鍵復号手段と、前記データをコンテンツ鍵で復号して、コンテンツを再生するコンテンツ再生手段とを備えることを特徴とする再生装置。

【請求項14】 前記再生装置は、記録媒体に記録されたコンテンツをコンテンツ鍵で暗号化したデータと、前記コンテンツ鍵を暗号化した暗号文と、暗号化に用いた鍵を識別する情報とを読み出し、前

記再生情報取得手段に与える読出手段を更に備えることを特徴とする請求項13記載の再生装置。

【請求項15】 前記再生装置は、鍵管理装置から送出されるコンテンツをコンテンツ鍵で暗号化したデータと、前記コンテンツ鍵を暗号化した暗号文と、暗号化に用いた鍵を識別する情報とを受信し、前記再生情報取得手段に与える受信手段を更に備えることを特徴とする請求項13記載の再生装置。

【請求項16】 暗号化されたデータを復号して再生する複数の再生装置に割り当てた鍵を管理する鍵管理装置の鍵管理方法であって、

木構造は少なくとも1つあり、木構造の第N層の鍵から最上層の鍵に辿る異なる経路上の鍵群は、それぞれ異なる再生装置に割り当てられており、N（Nは、2以上の自然数）層の木構造の各ノードに配置された鍵を鍵管理装置の記憶領域に記憶しており、

前記各鍵群のうち、1つの再生装置が有する鍵群の情報の通知を受け付ける受付ステップと、

当該鍵群の各鍵を無効鍵とし、無効鍵を経路上のノードに持つ他の再生装置に割り当てられた鍵群のうちから、前記無効鍵より一層下層の無効鍵でない鍵を選択する鍵選択ステップと、

前記データの暗号化に用いたコンテンツ鍵を当該選択した鍵で暗号化した暗号文と、当該選択した鍵を特定する特定情報とからなる暗号情報を生成する暗号情報生成ステップとを有し、

前記各再生装置は、割り当てられたN個の鍵を記憶しており、前記特定情報により特定される鍵を用いて対応する暗号文を復号してコンテンツ鍵を得、前記データをそのコンテンツ鍵で復号して、コンテンツを再生することを特徴とする鍵管理方法。

【請求項17】 暗号化されたデータを復号して再生する複数の再生装置に割り当てた鍵をコンピュータで管理する鍵管理プログラムであって、

木構造は少なくとも1つあり、木構造の第N層の鍵から最上層の鍵に辿る異なる経路上の鍵群は、それぞれ異なる再生装置に割り当てられており、N（Nは、2以上の自然数）層の木構造の各ノードに配置された鍵を記憶領域に記憶しており、

前記各鍵群のうち、1つの再生装置が有する鍵群の情報の通知を受け付ける受付ステップと、

当該鍵群の各鍵を無効鍵とし、無効鍵を経路上のノードに持つ他の再生装置に割り当てられた鍵群のうちから、前記無効鍵より一層下層の無効鍵でない鍵を選択する鍵選択ステップと、

前記データの暗号化に用いたコンテンツ鍵を当該選択した鍵で暗号化した暗号文と、当該選択した鍵を特定する特定情報とからなる暗号情報を生成する暗号情報生成ステップとを有し、

前記各再生装置は、割り当てられたN個の鍵を記憶して

おり、前記特定情報により特定される鍵を用いて対応する暗号文を復号してコンテンツ鍵を得、前記データをそのコンテンツ鍵で復号して、コンテンツを再生することとを特徴とする鍵管理プログラム。

【請求項18】 暗号化されたデータを復号して再生する複数の再生装置に割り当てた鍵を管理する鍵管理装置に適用されるコンピュータ読み取り可能な記録媒体は、木構造は少なくとも1つあり、木構造の第N層の鍵から最上層の鍵に辿る異なる経路上の鍵群は、それぞれ異なる再生装置に割り当てられており、N（Nは、2以上の自然数）層の木構造の各ノードに配置された鍵を記憶領域に記憶しており、

前記各鍵群のうち、1つの再生装置が有する鍵群の情報の通知を受け付ける受付ステップと、当該鍵群の各鍵を無効鍵とし、無効鍵を経路上のノードに持つ他の再生装置に割り当てられた鍵群のうちから、前記無効鍵より一層下層の無効鍵でない鍵を選択する鍵選択ステップと、

前記データの暗号化に用いたコンテンツ鍵を当該選択した鍵で暗号化した暗号文と、当該選択した鍵を特定する特定情報とからなる暗号情報を生成する暗号情報生成ステップとをコンピュータに実行させるプログラムを記録し、

前記各再生装置は、割り当てられたN個の鍵を記憶しており、前記特定情報により特定される鍵を用いて対応する暗号文を復号してコンテンツ鍵を得、前記データをそのコンテンツ鍵で復号して、コンテンツを再生することとを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項19】 書き換え可能な記録媒体に暗号化したデータを記録する複数の記録装置と、記録媒体に記録された暗号化されたデータを復号して再生する複数の再生装置と、前記記録装置と前記再生装置とに割り当てた鍵を管理する鍵管理装置とからなるシステムであって、

前記鍵管理装置は、木構造は少なくとも1つあり、木構造の第N層の鍵から最上層の鍵に辿る異なる経路上の鍵群は、それぞれ異なる記録装置と再生装置とに割り当てられているN（Nは、2以上の自然数）層の木構造の各ノードに配置された鍵を記憶している鍵記憶手段と、

前記各鍵群のうち、1つの記録装置及び／又は再生装置が有する鍵群の情報の通知を受けると、当該鍵群の各鍵を無効鍵とし、無効鍵を経路上のノードに持つ他の記録装置及び／又は再生装置に割り当てられた鍵群のうちから、前記無効鍵より一層下層の無効鍵でない鍵を選択し、前記データの暗号化に用いたコンテンツ鍵を当該選択した鍵で暗号化した暗号文と、当該選択した鍵を特定する特定情報とからなる暗号情報を生成する暗号情報生成手段と、

前記記録媒体に生成された暗号情報を記録する暗号情報記録手段とを備え、

前記記録装置は、

各鍵は、N（Nは、2以上の自然数）層の木構造の各ノードに配置された鍵の木構造の第N層の鍵から最上層の鍵に辿る異なる経路上の1つの経路上にある鍵であるN個の鍵を記憶している鍵群記憶手段と、

前記記録媒体から暗号情報を読み出し、暗号文を特定情報で特定される鍵記憶手段に記憶されている鍵データで復号してコンテンツ鍵を得るコンテンツ鍵復号手段と、取得したコンテンツを得られたコンテンツ鍵で暗号化したデータを前記記録媒体に記録するコンテンツ暗号化手段とを備え、

前記再生装置は、

各鍵は、N（Nは、2以上の自然数）層の木構造の各ノードに配置された鍵の木構造の第N層の鍵から最上層の鍵に辿る異なる経路上の1つの経路上にある鍵であるN個の鍵を記憶している鍵群記憶手段と、

コンテンツをコンテンツ鍵で暗号化したデータと、前記コンテンツ鍵を暗号化した少なくとも1つ以上の暗号文と、暗号化に用いた鍵を特定する特定情報とを取得する再生情報取得手段と、

前記特定情報で特定される鍵を前記鍵群記憶手段に記憶されている鍵から選択し、当該選択した鍵で対応する暗号文を復号してコンテンツ鍵を得るコンテンツ鍵復号手段と、

前記データをコンテンツ鍵で復号して、コンテンツを再生するコンテンツ再生手段とを備えることを特徴とする鍵管理システム。

【請求項20】 N（Nは、2以上の自然数）層の木構造の各ノードに配置された鍵の第N層の鍵から最上層の鍵に辿る異なる経路上の1つの鍵群を記憶している記録装置で、コンテンツをコンテンツ鍵で暗号化したデータが記録され、同様の他の1つの鍵群を記憶している再生装置で読み出されて暗号化されたデータがコンテンツ鍵で復号される書き換え可能な記録媒体であって、

前記コンテンツ鍵を暗号化した暗号文を記憶している暗号文領域と、

前記暗号化に用いた鍵を特定する情報が記憶されている選択鍵リスト領域と、

前記記録装置で記録されるデータののための領域であるデータ領域とを有し、

前記暗号文は少なくとも1つ以上あり、暗号化に用いた選択鍵は前記記録装置及び前記再生装置に記憶されている鍵群に含まれる1つの鍵と一致しており、前記データは、前記暗号文を前記鍵を特定する情報で特定された前記再生装置に記憶された選択鍵を用いて復号化されたコンテンツ鍵で復号されることを特徴とする書き換え可能な記録媒体。

【請求項21】 書き換え可能な記録媒体に暗号化したデータを記録する複数の記録装置と、記録媒体に記録された暗号化されたデータを復号して再生する複数の再生

装置とに割り当てた鍵を管理する鍵管理装置であって、木構造は少なくとも1つあり、木構造の第N層の鍵から最上層の鍵に辿る異なる経路上の鍵群は、それぞれ異なる記録装置と再生装置とに割り当てられているN（Nは、2以上の自然数）層の木構造の各ノードに配置された鍵を記憶している鍵記憶手段と、

前記各鍵群のうち、1つの記録装置及び／又は再生装置が有する鍵群の情報の通知を受けると、当該鍵群の各鍵を無効鍵とし、無効鍵を経路上のノードに持つ他の記録装置及び／又は再生装置に割り当てられた鍵群のうちから、前記無効鍵より一層下層の無効鍵でない鍵を選択し、前記データの暗号化に用いたコンテンツ鍵を当該選択した鍵で暗号化した暗号文と、当該選択した鍵を特定する特定情報とからなる暗号情報を生成する暗号情報生成手段と、

前記記録媒体に生成された暗号情報を記録する暗号情報記録手段とを備えることを特徴とする鍵管理装置。

【請求項22】 書き換え可能な記録媒体に暗号化したデータを記録する記録装置であって、

各鍵は、N（Nは、2以上の自然数）層の木構造の各ノードに配置された鍵の木構造の第N層の鍵から最上層の鍵に辿る異なる経路上の1つの経路上にある鍵であるN個の鍵を記憶している鍵群記憶手段と、

前記記録媒体から暗号情報を読み出し、暗号文を特定情報で特定される鍵群記憶手段に記憶されている鍵データで復号してコンテンツ鍵を得るコンテンツ鍵復号手段と、

取得したコンテンツを得られたコンテンツ鍵で暗号化したデータを前記記録媒体に記録するコンテンツ暗号化手段とを備え、

前記記録媒体には、前記データの暗号化に用いるコンテンツ鍵を当該選択した鍵で暗号化した暗号文と、当該選択した鍵を特定する特定情報とからなる暗号情報が記憶されていることを特徴とする記録装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、映画等の著作物であるコンテンツの著作権を保護するため、複数の再生装置に予め記憶された鍵群を管理する鍵管理装置及び鍵管理装置によりデータが記録された記録媒体、記録媒体から読み出されたデータ又は鍵管理装置から出力されたデータを再生する再生装置に関する。

【0002】

【従来の技術】近年、記録媒体が大容量化するに従い、映画等の著作物をデジタル化したコンテンツを例えばDVD等の記録媒体に格納して市販するビジネスが盛んに行なわれている。このようなビジネスにおいては、このDVDを再生する再生装置は、コンテンツの著作権を保護して、著作権者との合意による制限の下でのみコンテンツの再生や複製等を実行することが必要となる。

【0003】例えば、著作物を不正コピー等から保護するため、デジタルコンテンツは、ある暗号鍵により暗号化されてDVDに記録され、これを復号できるのは該当する復号鍵を持つ再生装置だけといった仕組みを備えている。この場合、再生装置が有する復号鍵は、外部に露見しないように、厳重に管理される必要があるが、何かの事故や事件により、ある再生装置の復号鍵が不正者によって暴露されることがある。ある再生装置の復号鍵が一旦不正者に暴露されてしまうと、この不正者は、この復号鍵を用いてコンテンツを復号し、著作権者の制御を逃れて、コンテンツを不正に扱う可能性がある。この不正使用された再生装置が有する復号鍵は、無効化する必要がある。

【0004】同様の問題は、衛星放送やインターネットのマルチキャストのような放送型メディアにおける受信装置が有する鍵にもある。衛星放送等では、暗号化された番組を受信装置が有する鍵で復号し、番組の再生を行っているけれども、受信者が有料番組の受信契約を解除した場合、当該受信装置が有する鍵を無効化しなければならない。この受信装置の有する鍵を個別に無効化する技術に、例えば、特開平11-187013号公報記載の暗号鍵配信システムがある。

【0005】

【発明が解決しようとする課題】ところが、この暗号鍵配信システムでは、各受信装置がN個の鍵、即ち、N層に階層化された木構造に配置された鍵の1つの経路の鍵群を有するときには、特定の一つの受信装置が有する鍵群を無効化するのに暗号文を2N-3個生成する必要がある。また、当該受信装置以外の受信装置では、最大N-1個の暗号文を順次復号して、コンテンツを暗号化したコンテンツ鍵を求める必要がある。

【0006】本発明は、上記課題に鑑み、再生装置の有する鍵を無効化するに際して、生成する暗号文を半減し、かつ、再生装置でコンテンツ鍵を取得するために復号する暗号文の数を最小とする鍵管理装置又は再生装置を提供することを第1の目的とする。また、本発明の第2の目的は、一旦無効化した鍵を再び用いることができるよう復帰することのできる鍵管理装置を提供することである。

【0007】

【課題を解決するための手段】上記課題を解決するため、本発明は、暗号化されたデータを復号して再生する複数の再生装置に割り当てた鍵を管理する鍵管理装置であって、木構造は少なくとも1つあり、木構造の第N層の鍵から最上層の鍵に辿る異なる経路上の鍵群は、それぞれ異なる再生装置に割り当てられているN（Nは、2以上の自然数）層の木構造の各ノードに配置された鍵を記憶している鍵記憶手段と、前記各鍵群のうち、1つの再生装置が有する鍵群の情報の通知を受けると、当該鍵群の各鍵を無効鍵とし、無効鍵を経路上のノードに持つ

他の再生装置に割り当てられた鍵群のうちから、前記無効鍵より一層下層の無効鍵でない鍵を選択し、前記データの暗号化に用いたコンテンツ鍵を当該選択した鍵で暗号化した暗号文と、当該選択した鍵を特定する特定情報とからなる暗号情報を生成する暗号情報生成手段とを備え、前記各再生装置は、割り当てられたN個の鍵を記憶しており、前記特定情報により特定される鍵を用いて対応する暗号文を復号してコンテンツ鍵を得、前記データをそのコンテンツ鍵で復号して、コンテンツを再生することとしている。

【0008】

【発明の実施の形態】以下、本発明に係る鍵管理装置及び再生装置の実施の形態について、図面を用いて説明する。

（実施の形態1）図1は、本発明に係る鍵管理装置及び再生装置の実施の形態1の構成図である。鍵管理装置101は、鍵管理情報記憶部111と、コンテンツ記憶部112と、コンテンツ鍵生成部113と、コンテンツ暗号化部114と、鍵選択部115と、受付部116と、暗号文生成部117と、選択鍵リスト生成部118と、記録部119とを備えている。

【0009】記録媒体102は、大容量の記憶領域を有するDVD等からなる。再生装置103は、鍵記憶部131と、読出部132と、鍵選択部133と、コンテンツ鍵復号部134と、コンテンツ復号部135と、再生部136とを備えている。鍵管理情報記憶部111は、図2に示すような木構造の各ノードに配置された各鍵を鍵管理情報として記憶している。この木構造は、2進木であり、5層に階層化され、最上層のレイヤ1から最下層のレイヤ5までである。

【0010】レイヤ5の各鍵は、各再生装置103の個別鍵であり、レイヤ5の各個別鍵からレイヤ1の鍵KeyOに辿る経路上の鍵群は、各再生装置103にそれぞれ割り当てられている。例えば、再生装置1には、個別鍵IK1、鍵KeyA、KeyI、KeyM、KeyOの5個の鍵が割り当てられている。同様に、再生装置7には、個別鍵IK7、鍵KeyD、KeyJ、KeyM、KeyOの5個の鍵が割り当てられている。

【0011】図3は、鍵管理情報記憶部111に記憶されている鍵管理情報を示している。鍵管理情報301には、鍵ID302と、鍵データ303と、親鍵のID304と、鍵状態305とが記載されている。鍵ID302は、図2に示した木構造の各ノードに配置された各鍵を識別する識別子である。

【0012】鍵データ303は、任意に生成されたものであり、鍵管理装置101で用いられるときには、暗号鍵となり、再生装置103で用いられるときには、復号鍵となる。親鍵のID304は、各鍵の一層上層のレイヤの鍵の識別子である。例えば、個別鍵IK1の親鍵のID304は、KeyAである。なお、レイヤ1のKe

yOには、親鍵が存在しないので、“11・・・11”と記載され、親鍵がないことが示されている。

【0013】鍵状態305は、現在の鍵の使用状態を示すものであり、コンテンツ鍵の暗号化又は復号化に用いられている鍵を選択鍵「1」で示している。また、鍵状態305が「0」の鍵は、暗号鍵又は復号鍵に用いられていない未使用鍵を示している。鍵管理情報301は、鍵管理情報の初期状態であり、鍵状態305に「-1」は存在しない。鍵状態305が「-1」の鍵は、後述する無効鍵である。

【0014】コンテンツ記憶部112は、ハードディスク等からなり、映画等の著作物をデジタル化したコンテンツを記憶している。コンテンツ鍵生成部113は、コンテンツ毎にコンテンツを暗号化するコンテンツ鍵を生成する。なお、鍵管理情報301等が更新されたとき、コンテンツ毎にコンテンツ鍵を更新する。

【0015】コンテンツ暗号化部114は、DES等の共通鍵暗号化方式によって、コンテンツを暗号化する。コンテンツ暗号化部114は、暗号化指示を受付部116から通知されると、コンテンツ記憶部112から読み出したコンテンツをコンテンツ鍵生成部113で生成されたコンテンツ鍵で暗号化して、記録部119に通知する。

【0016】鍵選択部115は、受付部116から暗号化指示を通知されると、鍵管理情報記憶部111に記憶されている鍵管理情報301の鍵状態305に「1」が記載されている鍵を見つける。当該鍵の鍵ID302と鍵データ303とを読み出し、暗号文生成部117に通知し、当該鍵の鍵ID302を選択鍵リスト生成部118に通知する。

【0017】鍵選択部115は、受付部116から無効にすべき鍵IDを通知されると、鍵管理情報記憶部111に記憶されている鍵管理情報301を更新する。今、図2に示した再生装置7に割り当てられている鍵群IK7、KeyD、KeyJ、KeyM、KeyOを無効にすべき鍵IDとして通知されると、鍵管理情報301に記載された各鍵について、まず、鍵状態305が「-1」の鍵を除外する。ここで、鍵状態「-1」は、不正に使用された再生装置に割り当てられた鍵を示しており、この鍵を無効鍵という。

【0018】次に、鍵選択部115は、鍵ID302と通知された鍵IDとが一致するか否かを順に判定する。鍵ID302と通知された鍵IDとが一致するときには、鍵状態を「-1」に更新する。一致しないとき、当該鍵の親の鍵の鍵状態が「-1」か否かを判定し、「-1」でなければ鍵状態305を未使用鍵を示す「0」のままにし、「-1」のときには、自身の鍵状態305を「1」に更新する。鍵状態「1」は、コンテンツ鍵の暗号化に用いられることを示しており、この鍵を選択鍵という。この処理を鍵管理情報301に記載された全ての

鍵について行なう。

【0019】鍵選択部115は、この処理によって、鍵管理情報301を図4に示す鍵管理情報401に更新する。次に、鍵選択部115は、鍵状態305が「1」の鍵ID302と鍵データ303とを暗号文生成部117に通知し、鍵状態305が「1」の鍵ID302を選択鍵リスト生成部118に通知する。

【0020】なお、鍵選択部115は、全ての無効にすべき鍵の鍵IDの通知をうけることとしたけれども、無効にすべき個別鍵の鍵IDを1つ通知されてもよい。この場合、鍵選択部115は、通知された鍵IDに一致する鍵管理情報301、401の鍵ID302を見つけ、その親鍵のID304を順に辿ることによって、無効にすべき全ての鍵を知ることができる。

【0021】受付部116は、オペレータからコンテンツの暗号化の指示や、無効にすべき鍵IDの入力を受け付ける。コンテンツの暗号化指示を受け付けると、鍵選択部115とコンテンツ暗号化部114にその旨を通知する。無効にすべき鍵IDの入力を受け付けると、入力された鍵IDを鍵選択部115に通知する。暗号文生成部117は、鍵選択部115から鍵IDと鍵データとの通知を受けると、コンテンツ鍵生成部113で生成されたコンテンツ鍵を通知された鍵データで暗号化した暗号文を生成する。生成した暗号文を記録部119に通知する。

【0022】選択鍵リスト生成部118は、鍵選択部115から通知された鍵IDの一覧を選択鍵リストとして生成し、記録部119に通知する。記録部119は、コンテンツ暗号化部114から通知された暗号化されたコンテンツと、暗号文生成部117から通知された暗号文と、選択鍵リスト生成部118から通知された選択鍵リストとを記録媒体102の各記憶領域に記録する。

【0023】記録媒体102には、選択鍵リスト記憶領域と暗号文記憶領域とデータ記憶領域が用意されており、記録部119によって、選択鍵リスト、暗号文及びコンテンツ鍵で暗号化されたコンテンツがそれぞれ記録される。図5は、図3に示す鍵管理情報301が鍵管理情報記憶部111に記憶されているときに、記録媒体102に記録される記録内容を示している。

【0024】記録内容501には、コンテンツをコンテンツ鍵で暗号化したデータ502と、コンテンツ鍵を鍵管理情報301の鍵状態305が「1」の鍵、即ち、木構造の最上層のレイヤ1の鍵KeyOで暗号化した暗号文503と、暗号文503の暗号化に用いた鍵を特定する選択鍵リスト504とが含まれている。なお、E(X, Y)は、データYを鍵Xで暗号化していることを示し、暗号文503は、コンテンツ鍵を鍵ID「KeyO」の鍵データで暗号化したことを示している。

【0025】図6は、再生装置7（図2参照）に割り当てられた鍵群、IK7、KeyD、KeyJ、Key

M、KeyOが無効鍵とされた後に、記録媒体102に記録される記憶内容を示している。即ち、図4に示す鍵管理情報401が鍵管理情報記憶部111に記憶されているときの記録内容を示している。記録内容601には、データ602と、暗号文603と選択鍵リスト604とが含まれている。

【0026】データ602には、コンテンツをコンテンツ鍵で暗号化したデータが記録されている。コンテンツ鍵は、コンテンツ毎に生成されており、又、鍵管理情報301等が更新されたときには、同一のコンテンツに対しても新たなコンテンツ鍵が生成されている。このため、記録内容501と記録内容601とのそれぞれのデータ502、602は、コンテンツが同一であっても、コンテンツ鍵が異なるので同一データとはならない。

【0027】暗号文603は、コンテンツ鍵を選択鍵リスト604に記録した各鍵で暗号化したものである。記録内容501では、選択鍵リスト504に記録された鍵が1個であるので暗号文503も1個であるけれども、記録内容601では、選択鍵リスト604に記録された鍵が、4個であるので暗号文603も4個となる。因みに、従来技術で引用した暗号鍵配信システムでは、1個の個別鍵とその上位層の親鍵を無効としたとき、本実施の形態と同様に5層の木構造であれば、暗号文は7個である。引例の暗号鍵配信システムでは、N層の木構造（2進木）では、2N-3個の暗号文が必要であるけれども、本実施の形態では、N-1個の暗号文が必要となるだけである。

【0028】次に、再生装置103について説明する。鍵記憶部103は、図2に示した木構造の各ノードに配置された鍵を予め割り当てられており、鍵IDと鍵データとを対とした5個の鍵情報を記憶している。図7は、図2に示した再生装置1の鍵記憶部131に記憶されている鍵情報を示している。鍵情報701には、鍵ID702と鍵データ703とが対にして記載されている。

【0029】読出部132は、記録媒体102が再生装置103に装着され、記録媒体102の再生指示を操作部（図示せず）から通知されると、記録媒体102から記録内容を読み出す。読出部132は、読み出した記録内容のうち、選択鍵リストを鍵選択部133に、暗号文をコンテンツ鍵復号部134に、暗号化されたコンテンツであるデータをコンテンツ復号部135にそれぞれ通知する。

【0030】鍵選択部133は、選択鍵リストを通知されると、選択鍵リストに記載された鍵IDと一致する鍵記憶部131に記憶されている鍵情報の鍵IDを選択する。選択した鍵IDと鍵データとを読み出し、コンテンツ鍵復号部134に通知する。コンテンツ鍵復号部134は、鍵選択部133から通知された鍵IDに対応する読出部132から通知された暗号文を鍵選択部133から通知された鍵データを復号鍵として復号する。復号さ

れたコンテンツ鍵をコンテンツ復号部135に通知する。

【0031】コンテンツ復号部135は、コンテンツ鍵復号部134から通知されたコンテンツ鍵の正当性を署名等の方法で確認する。次に、読出部132から通知された暗号化されたコンテンツをコンテンツ鍵復号部134から通知されたコンテンツ鍵で復号する。復号したコンテンツを再生部136に通知する。再生部136は、コンテンツ復号部135から通知されたコンテンツを再生して出力する。

【0032】今、具体例として再生装置103が図2に示した再生装置1であり、記録媒体102に記録内容501が記録されている場合について説明する。鍵記憶部131には、鍵情報701が記憶されており、鍵選択部133には、読出部132から選択鍵リスト504の鍵ID「KeyO」が通知される。鍵選択部133は、この鍵ID「KeyO」と一致する鍵ID「KeyO」を鍵情報701から選択し、その鍵ID702の「KeyO」と鍵データとを読み出し、コンテンツ鍵復号部134に通知する。

【0033】コンテンツ鍵復号部134は、読出部132から通知された暗号文を鍵選択部133から通知された鍵データで復号してコンテンツ鍵を得る。このコンテンツ鍵をコンテンツ復号部135に通知する。次に、記録媒体に記録内容601が記録されている場合では、鍵選択部133には、読出部132から選択鍵リスト604の鍵ID「KeyN, KeyI, KeyC, IK8」が通知される。

【0034】鍵選択部133は、鍵記憶部702に記憶されている鍵情報701の鍵ID「KeyI」が一致するので選択する。選択した鍵ID「KeyI」とその鍵データとを読み出し、コンテンツ鍵復号部134に通知する。コンテンツ鍵復号部134では、通知された4つの暗号文のうち、「KeyI」で暗号化された暗号文604を鍵選択部133から通知された鍵データで復号し、コンテンツ鍵を得る。

【0035】図2に示した再生装置7では、記録媒体102に記録内容601が記録されている場合、鍵選択部133に通知された選択鍵リスト604の鍵ID「KeyN, KeyI, KeyC, IK8」と鍵記憶部131に記録されている鍵ID「IK7, KeyD, KeyJ, KeyM, KeyO」とでは、一致する鍵IDが存在しない。したがって、コンテンツ鍵復号部134で暗号文を復号化してコンテンツ鍵を得ることができない。

【0036】因みに、本実施の形態では、コンテンツ鍵を得るためにコンテンツ鍵復号部134が復号する暗号文は、不正使用された再生装置7を除き、全て1個であるけれども、従来技術で引用した暗号鍵配信システムでは、本実施の形態と同様に5層の木構造である場合に、コンテンツ鍵を取得するまでに、最大4個、即ち、N-

1個の暗号文を復号する必要がある。

【0037】次に、本実施の形態の主要な動作である鍵管理装置101における鍵管理情報の更新処理を図8のフローチャートを用いて説明する。まず、鍵選択部115は、受付部116から不正使用に供された再生装置に割り当てられた無効にすべき鍵の鍵IDの通知を待ち、(s802)、カウンタiを「1」に初期化する(s804)。次に、カウンタjを「1」に初期化する(s806)。

10 【0038】鍵選択部115は、鍵管理情報記憶部111に記憶されている鍵管理情報の第i層(レイヤi)のj番目の鍵状態が「-1」であるか否かを判定する(s808)。「-1」であればs818に移る。「-1」でなければ、鍵管理情報のレイヤiのj番目の鍵IDと通知された各鍵IDとが一致するか否かを判定する(s810)。一致しなければ、親の鍵(レイヤi-1)の鍵状態が「-1」か否かを判定する。なお、親の鍵がなければ否である(s812)。「-1」でなければs818に移る。「-1」のときには、自身の鍵状態を「0」から「1」に更新し(s814)、s818に移る。s810において、一致するときには、自身の鍵状態を「-1」にし(s816)、s818に移る。

20 【0039】次に、s818において、鍵選択部115は、カウンタjが2j-1か否かを判定し、否のときには、カウンタjに「1」を加え(s820)、s808に戻る。肯定のときには、カウンタiに「1」を加え(s822)、i>Nか否、即ち、カウンタiの値がレイヤNを超えたか否かを判定する(s824)。肯定のときには処理を終了し、否のときにはs806に戻る。

30 【0040】なお、本実施の形態では、図2に示した2進木のN層の木構造の各ノードに各鍵が配置されている場合について説明したけれども、3進木以上であってもよいし、各ノードが一定数でなくともよい。また、本実施の形態で、図2に示した再生装置7に割り当てられた鍵を無効とした後に、更に別の再生装置、例えば再生装置12に割り当てられた鍵を無効とする場合、鍵選択部115によって、図8に示した鍵管理情報更新処理の動作がなされ、鍵管理情報が更新される。

40 【0041】これによって、選択鍵リスト生成部118で、選択鍵リスト(KeyI, KeyL, KeyC, KeyE, IK8, IK11)が生成される。また、暗号文生成部117によって、以下の暗号文が生成される。
E(KeyI, コンテンツ鍵)
E(KeyL, コンテンツ鍵)
E(KeyC, コンテンツ鍵)
E(KeyE, コンテンツ鍵)
E(IK8, コンテンツ鍵)
E(IK11, コンテンツ鍵)

50 なお、本実施の形態において、鍵管理情報の初期状態である鍵管理情報301や再生装置7の有する鍵群を無効

化した際の鍵管理情報401や更に再生装置12の有する鍵群を無効化した際の鍵管理情報(図示せず)をその更新日時とともに記憶するようにしてもよい。

【0042】このように鍵管理情報301等の履歴を鍵管理情報記憶部111に記憶しておけば、鍵状態305等を容易に過去のある状態まで戻すことができる。

(実施の形態2)次に、本発明に係る鍵管理装置及び再生装置の実施の形態2について説明する。この鍵管理装置及び再生装置は、上記実施の形態1の構成とほぼ同様であるので、図1に示した構成図を用いて説明する。

【0043】本実施の形態では、各再生装置に割り当てられる鍵を複数の木構造の各ノードに配置された鍵群としている。鍵管理情報記憶部111は、図9に示すよう4個の木構造の各ノードに配置された各鍵を鍵管理情報として記憶している。各木構造901、902、903、904は、3層に階層化された2進木の構造であり、レイヤ3の鍵は、各再生装置の個別鍵である。例えば、再生装置1には、個別鍵IK1とその上位層のKeyAとKeyIとが割り当てられている。同様に、再生装置2には、個別鍵IK2とその上位層のKeyAとKeyIとが割り当てられている。

【0044】これらの各鍵の鍵管理情報を図10に示す。鍵管理情報1001には、鍵管理情報301と同様に鍵ID1002と鍵データ1003と親鍵のID1004と鍵状態1005とが含まれており、木構造901のレイヤ1からレイヤ3、次に木構造902のレイヤ1からレイヤ3の順に、更に、木構造904のレイヤ3までの各鍵について記載されている。

【0045】この鍵管理情報1001には、選択鍵、即ち鍵状態1005の「1」の鍵が4個ある。したがって、暗号文生成部117で生成される暗号文は、4個となる。上記実施の形態1と同様に、再生装置7に割り当てられた鍵を無効化した場合、選択鍵は、KeyI、KeyC、IK8、KeyK、KeyLの5個となる。更に再生装置12に割り当てられた鍵を無効化した場合、選択鍵は、KeyI、KeyC、IK8、KeyE、IK11、KeyLの6個となる。したがって暗号文はそれぞれ5個と6個となる。

【0046】なお、鍵管理情報の更新処理の動作は、上記実施の形態1の動作を説明した図8のフローチャートが、1本の木構造についての処理であるので、L本の木構造であれば、s802～s824をL回繰り返すようにすればよい。図11は、再生装置103の数を16とした場合の木構造の数の相違による鍵管理情報に基づく諸データの比較表を示している。

【0047】比較表1101には、木構造の数1102と鍵数1103と、不正使用された再生装置1104と、選択鍵数=暗号文数1105と、再生装置での鍵数1106とが記載されている。木構造の数1102は、上記実施の形態1では、「1」とし、本実施の形態では

「4」としている。木構造の数1102を増加させれば、階層化の層の数が減少し、その分、鍵数1103も減少する。従って、木構造の数1102を増加させれば、鍵管理情報記憶部111に記憶させる鍵数も減少する。また、各再生装置103の鍵記憶部131で記憶している鍵数1106も減少する。

【0048】ところが、木構造の数1102が増加すると、コンテンツ鍵を暗号化する選択鍵数=暗号文数1105が初期状態で増加する。ここで、初期状態とは、不正使用された再生装置数1104が「0」の状態をいう。不正使用された再生装置の有する鍵群を無効鍵とした場合、不正使用された再生装置数1104が増加すると、暗号文数1105も増加するけれども、木構造の数1102により、増加割合は異なる。例えば、不正使用された再生装置数1104が「2」のときには、木構造の数1102が「1」、「2」、「4」とも暗号文数1105は「6」となる。

【0049】以上のことから、無効とする鍵群の数の最大値を2Kとすると、木構造の数Lを2K+1と設定すると、暗号文数1105や再生装置での鍵数1106や鍵管理情報記憶部111に記憶する鍵数1103等を最小にすることができる。

(実施の形態3)図12は、本発明に係る鍵管理装置と再生装置との実施の形態3の構成図である。

【0050】鍵管理装置1201は、鍵管理情報記憶部111と、コンテンツ記憶部112と、コンテンツ鍵生成部113と、コンテンツ暗号化部114と、鍵選択部1211と、受付部116と、暗号文生成部117と、選択鍵リスト生成部118と、多重化送出部1212とを備えている。再生装置1202は、受信部1221と、鍵記憶部131と、鍵選択部133と、コンテンツ鍵復号部134と、コンテンツ復号部135と、再生部136とを備えている。上記実施の形態1の鍵管理装置101及び再生装置103と同一の構成部分には同一の符号を付し、その説明を省略し、本実施の形態固有の構成部分について説明する。

【0051】本実施の形態の鍵管理装置1201は、上記実施の形態1の鍵管理装置101の記録部119に替えて、多重化送出部1212を備え、データ送出装置の機能を有する。再生装置1202は、上記実施の形態1の再生装置103の読出部132に替えて、受信部1221を備え、データ受信装置の機能を有する。

【0052】コンテンツ暗号化部114は、コンテンツ記憶部112からコンテンツを読み出し、コンテンツ鍵生成部113で生成されたコンテンツ鍵でコンテンツを暗号化したデータを多重化送出部1212に通知する。暗号文生成部117は、鍵選択部1211から通知された鍵データでコンテンツ鍵生成部113で生成されたコンテンツ鍵を暗号化した暗号文を生成し、多重化送出部1212に通知する。

【0053】選択鍵リスト生成部118は、鍵選択部1211から通知された鍵IDの一覧を選択鍵リストとして生成し、多重化送出部1212に通知する。多重化送出部1212は、コンテンツ暗号化部114から通知されたデータと、暗号文生成部117で生成された暗号文と、選択鍵リスト生成部118で生成された選択鍵リストとを複数の再生装置1202に送出する。

【0054】再生装置1202の受信部1221は、多重化送出部1212から送出されたデータと暗号文と選択鍵リストとを受信し、データをコンテンツ復号部135に、暗号文をコンテンツ鍵復号部134に、選択鍵リストを鍵選択部133にそれぞれ通知する。なお、多重化送出部1212から受信部1221のデータ等の送出は、放送波によるものであってもよいし、公衆回線網を介したインターネットのマルチキャストの通信路を用いてもよいし、CATV等であってもよい。

【0055】各再生装置1202は、契約により鍵管理装置1201からデータを受信しているものとし、契約の解除によって上記実施の形態1の不正に使用された再生装置103と同様に再生装置1202の有する鍵群が無効鍵とされる。鍵管理情報記憶部111は、上記実施の形態1と同様に図2に示すような木構造の各ノードに配置された鍵を鍵管理情報として記憶している。

【0056】今、再生装置7と再生装置12との有する鍵群を契約の解除により一旦無効とした後に、再度、再生装置12が契約を復活した場合、再生装置12の有する鍵群を復帰させる処理について説明する。図13は、一旦無効化された鍵を再度利用できるように復帰する動作を説明するフローチャートである。

【0057】受付部116は、オペレータから再生装置12が有する鍵群の鍵ID「KeyO, KeyN, KeyK, KeyF, IK12」の入力を受け付ける。鍵選択部1211は、受付部116からの「KeyO, KeyN, KeyK, KeyF, IK12」の通知を待ち、(s1302)、カウンタiに初期値「1」を設定し(s1304)、カウンタjに初期値「1」を設定する(s1306)。

【0058】鍵選択部1211は、レイヤ1の1番目の鍵ID「KeyO」と通知された鍵IDとが一致するか否かを判定する(s1308)。否の場合は、この木構造ではないので、処理を終了し、別の木構造の鍵管理情報との照合に移る。本実施の形態では、木構造は1つであり、通知された鍵IDと一致するので、レイヤ1の1番目の鍵を共通の親鍵とする鍵の鍵状態は共に「-1」か否かを判定する(s1310)。「KeyM」と「KeyN」とは共に鍵状態が「-1」であるので、s1314に移る。もし、いずれかの鍵状態が「-1」でなければ、即ち、「KeyM」の鍵状態が「1」であれば、レイヤ1の1番目の鍵の鍵状態を「1」に更新する(s1312)。

【0059】次に、鍵選択部1211は、カウンタiに「1」を加え(s1314)、レイヤiのj番目の鍵IDと通知された鍵IDとが一致するか否かを判定し(s1316)、一致するとき、親鍵の鍵状態が「-1」であるか否かを判定する(s1317)。s1316でレイヤiのj番目の鍵IDと通知された鍵IDとが一致しないと判定されたとき、親鍵の鍵状態が「1」に更新されたか否かを判定し(s1318)、更新されていなければs1324に移り、更新されているときには、レイヤiのj番目の鍵の鍵状態を「0」に更新し(s1322)、s1324に移る。

【0060】鍵選択部1211は、s1317で親鍵の鍵状態が「-1」でないと判定したとき、s1322に移り、「-1」であるとき、レイヤiのj番目の鍵の鍵状態を「1」に更新し(s1320)、s1324に移る。鍵選択部1211は、s1324において、カウンタjの値が2i-1であるか否かを判定し、否であればカウンタj「1」を加え(s1326)、s1316に戻り、肯定であればカウンタiの値が「N」であるか否かを判定する(s1328)。肯定であれば処理を終了し、否であればカウンタjを「1」に初期化して(s1330)、s1314に戻る。

【0061】このような処理の結果、再生装置12の有する鍵群が復帰され、鍵管理情報は、図4に示した鍵管理情報401に更新される。この結果、再生装置12では、鍵管理装置1201から送出される暗号文を鍵記憶部131に記憶された鍵データで復号してコンテンツ鍵を得ることができる。このコンテンツ鍵を復号鍵として暗号化されたデータを復号し、再生することができる。

【0062】次に、新たな受信契約により、再生装置1202に割り当てる鍵群を鍵管理情報に追加する場合について説明する。今、鍵管理情報401の状態で4つの再生装置を追加する場合、鍵選択部1211は、新たに3層の木構造の鍵を生成する。図14は、この状態を説明する模式図である。新たな木構造1402は、再生装置17、18、19、20にそれぞれ対応する個別鍵IK17、IK18、IK19、IK20と、その上層のレイヤ2の鍵KeyP、KeyQと、最上層のレイヤ1のKeyRとからなる。

【0063】次に、鍵選択部1211は、レイヤ1のKeyRを既に在る木構造1401のレイヤ2のKeyN(KeyNの鍵状態は「-1」でない)に更新する。これによって、各再生装置17、18、19、20にそれぞれ割り当てられる鍵群は、以下ようになる。

再生装置17(KeyO, KeyN, KeyP, IK17)

再生装置18(KeyO, KeyN, KeyP, IK18)

再生装置19(KeyO, KeyN, KeyQ, IK19)

再生装置20(KeyO, KeyN, KeyQ, IK20)

鍵選択部1211は、鍵管理情報401に追加した鍵の鍵ID、鍵データ、親鍵のID、鍵状態を追加して記載する。なお、鍵状態は、「0」の未使用鍵とする。

【0064】ここでは、新たな木構造1402の親鍵KeyRを既存の木構造1401のKeyNに更新したけれども、KeyLに更新してもよい。

(実施の形態4)図15は、本発明に係る鍵管理装置と暗号情報記録装置と記録装置と再生装置とからなるシステムの実施の形態4の概略構成図である。

【0065】このシステムは、鍵管理装置1501と暗号情報記録装置1502と、複数の記録装置1503と、複数の再生装置1504とから構成され、書き換え可能な記録媒体1505には、予め暗号情報記録装置1502によって、暗号情報が記録されている。鍵管理装置1501は、上記実施の形態1の鍵管理装置101のコンテンツ記憶部112とコンテンツ暗号化部114と記録部119とを除外した構成であり、暗号情報記録装置1502は、鍵管理装置101の記録部119の一部によって構成される。

【0066】記録媒体1505は、DVD-RAM、DVD-RW等の書き換え可能な大容量の記録媒体であり、記録媒体の製造時に暗号情報記録装置によって選択鍵リストと暗号文とが記録される。記録装置1503は、図16に示すように、鍵記憶部1601とコンテンツ鍵復号部1602と暗号化部1603とを備えている。

【0067】鍵記憶部1601は、上記実施の形態1の再生装置103の鍵記憶部131と同様、予め割り当てられたN個の鍵を記憶している。記録装置1503に記録媒体1505が装着されると、コンテンツ鍵復号部1602は、記録媒体1505に記録された選択鍵リストと暗号文とを読み出す。選択鍵リストに記載された鍵IDの鍵データを鍵記憶部1601から読み出し、対応する暗号文を当該鍵データで復号してコンテンツ鍵を得る。得られたコンテンツ鍵を暗号化部1603に通知する。

【0068】暗号化部1603は、受信されたTV番組等のコンテンツを取得し、当該コンテンツを通知されたコンテンツ鍵で暗号化し、記録媒体1505に暗号化コンテンツ1605を記録する。次に、再生装置1504は、上記実施の形態1の再生装置103と同様の構成であり、図17に簡略化した構成を示している。

【0069】記録媒体1505が装着されると、コンテンツ鍵復号部1702は、選択鍵リストと暗号文とを記録媒体1505から読み出し、選択鍵リストに記録された鍵データを鍵記憶部1701から読み出す。読み出した鍵データで対応する暗号文を復号し、コンテンツ鍵を得る。得られたコンテンツ鍵を復号部1703に通知す

る。

【0070】復号部1703は、記録媒体から暗号化コンテンツを読み出し、通知されたコンテンツ鍵で復号し、再生して出力する。以上説明したように、上記実施の形態1、2では、読み出し専用の記録媒体102へ暗号化されたデータとその暗号情報とを記録することと説明したけれども、本実施の形態では、書き換え可能な記録媒体1505に予め暗号情報を記録しておき、その暗号情報に記録されたコンテンツ鍵を暗号化した暗号文を記録装置1503と再生装置1504とでそれぞれ復号してコンテンツ鍵を得るようにしている。記録装置1503では、そのコンテンツ鍵を用いてコンテンツを暗号化し、再生装置1504では、暗号化されたコンテンツをそのコンテンツ鍵を用いて復号するようにしている。

【0071】このようにして、このシステムでは、記録装置1503と再生装置1504とに割り当てられた鍵群を管理するようにしている。なお、上記各実施の形態において、鍵管理装置及び再生装置は、図1又は図12等の構成図で示したけれども、各構成要素の機能をコンピュータに発揮させるプログラムとして実現してもよい。更に、このプログラムをコンピュータ読み取り可能な記録媒体に記録しておき、鍵管理装置及び再生装置に適用することができる。

【0072】

【発明の効果】以上説明したように、本発明は、暗号化されたデータを復号して再生する複数の再生装置に割り当てた鍵を管理する鍵管理装置であって、木構造は少なくとも1つあり、木構造の第N層の鍵から最上層の鍵に辿る異なる経路上の鍵群は、それぞれ異なる再生装置に割り当てられているN(Nは、2以上の自然数)層の木構造の各ノードに配置された鍵を記憶している鍵記憶手段と、前記各鍵群のうち、1つの再生装置が有する鍵群の情報の通知を受けると、当該鍵群の各鍵を無効鍵とし、無効鍵を経路上のノードに持つ他の再生装置に割り当てられた鍵群のうちから、前記無効鍵より一層下層の無効鍵でない鍵を選択し、前記データの暗号化に用いたコンテンツ鍵を当該選択した鍵で暗号化した暗号文と、当該選択した鍵を特定する特定情報とからなる暗号情報を生成する暗号情報生成手段とを備え、前記各再生装置は、割り当てられたN個の鍵を記憶しており、前記特定情報により特定される鍵を用いて対応する暗号文を復号してコンテンツ鍵を得、前記データをそのコンテンツ鍵で復号して、コンテンツを再生することとしている。

【0073】このような構成によって、或る再生装置が有する鍵群を無効としたときに、他の再生装置では、1つの暗号文を自身の有するいずれかの鍵で復号してコンテンツ鍵を得ることができる。また、前記暗号情報生成手段は、コンテンツをコンテンツ鍵で暗号化したデータを生成するデータ生成部と、1つの再生装置に割り当てられた鍵群の情報の通知を受け付ける無効鍵受付部と、

通知された鍵群に含まれる各鍵を無効鍵とし、無効鍵の第N層を除く一層下層の異なる経路上の無効鍵でない鍵を選択鍵として選択する鍵選択部と、前記コンテンツ鍵を前記各選択鍵で暗号化した暗号文を生成する暗号文生成部と、前記各選択鍵を識別するリストを生成する選択鍵リスト生成部とを有することとしている。

【0074】このような構成によって、或る再生装置が有する無効とすべき鍵群の通知を受けると、他の再生装置では、復号することのできるコンテンツ鍵を暗号化した暗号文を生成する。また、データは、このコンテンツ鍵で暗号化されているので、他の再生装置では、暗号文を復号してコンテンツ鍵を得て、暗号化されたデータをコンテンツ鍵で復号することができる。しかし、無効化された鍵群を有する再生装置では、コンテンツ鍵を得ることができない。

【0075】また、前記鍵管理装置の鍵記憶手段は、各鍵ごとに、その鍵を識別する識別子と、その鍵の経路上の一層分上層の親鍵を識別する識別子と、その鍵が前記暗号文の生成に用いられている選択鍵か、無効鍵か、そのいずれでもない未使用鍵かの状態を示す鍵状態情報と、鍵データとを記載した鍵管理情報を記憶している鍵管理情報記憶部を有し、前記無効鍵受付部は、鍵群の各鍵の識別子を通知され、前記鍵選択部は、前記鍵管理情報の各鍵の識別子と通知された識別子とが、一致するとき前記鍵状態情報を無効鍵に更新し、一致しないとき親鍵が無効鍵であって自身が無効鍵でも選択鍵でもない未使用鍵のとき前記鍵状態情報を選択鍵に更新することとしている。

【0076】このような構成によって、鍵管理情報に記載された各鍵ごとの鍵状態情報を更新することによって、無効とすべき鍵群を確実に無効化することができる。また、前記鍵管理情報において、最上層の鍵の親鍵を識別する識別子には、特定の値が記載され、前記鍵選択部は、識別子に特定の値が記載された鍵の鍵情報が無効鍵でないときに選択鍵とすることとしている。

【0077】このような構成によって、初期状態では、木構造の最上層の鍵を用いてコンテンツ鍵を暗号化した暗号文を生成することができる。また、本発明の第2の目的は、前記暗号情報生成手段は、一旦無効鍵とした鍵で復帰させるべき1つの再生装置が有する鍵群の情報の通知を受け付ける復帰鍵受付手段と、通知された鍵群に含まれる鍵の経路上の一層上層の親鍵が無効鍵であり、その親鍵を共通の親鍵とする異なる経路上の鍵が共に無効鍵であるとき、その通知された鍵群に含まれる鍵を選択鍵とし、その選択鍵より下層の同一の経路上の鍵群の各鍵を選択鍵でも無効鍵でもない未使用鍵とする鍵復帰部とを更に有することとしている。

【0078】このような構成によって、一旦無効とした鍵群も再度、復帰させることができる。また、前記鍵記憶手段は、各鍵ごとに、その鍵を識別する識別子と、そ

の鍵の経路上の一層上層の親鍵を識別する識別子と、その鍵が前記暗号文の生成に用いられている選択鍵か、無効鍵か、そのいずれでもない未使用鍵かの状態を示す鍵状態情報と、鍵データとを記載した鍵管理情報を記憶している鍵管理情報記憶部を有し、前記復帰鍵受付部は、鍵群の各鍵の識別子を通知され、前記鍵復帰部は、前記鍵管理情報の各鍵の識別子と通知された識別子とが一致する場合、当該鍵が最上層の鍵であるとき、一層下層の異なる経路上の鍵が選択鍵であるとき、鍵状態情報を選択鍵に更新し、当該鍵が最上層の鍵以外であるとき、当該鍵の親鍵を共通にする異なる経路上の鍵が共に無効鍵であるとき、当該鍵の鍵状態情報を選択鍵に更新し、その選択鍵より下層の同一経路上の通知された識別子を有する各鍵の鍵状態情報を無効鍵、選択鍵のいずれでもない未使用鍵に更新し、通知された識別子と一致しない場合、その親鍵の鍵状態情報を選択鍵に更新したとき、鍵状態情報を未使用鍵に更新することとしている。

【0079】このような構成によって、復帰すべき鍵群の識別子を受け付けて、鍵管理情報を更新することができる。また、前記鍵管理装置は、新たに鍵群を割り当てる再生装置数を受け付ける新規受付手段と、木構造の第M層の鍵数を、再生装置数以上とするM(Mは2以上N以下の自然数)層の木構造の各ノードに配置された鍵を生成する新規鍵生成手段と、前記新規鍵生成手段で生成された木構造の最上層の鍵を既に鍵記憶手段に記憶されている(N-M+1)層以上の選択鍵又は未使用鍵に変更する接続手段とを更に備えることを特徴とする請求項2記載の鍵管理装置。こととしている。

【0080】このような構成によって、新たな鍵群を再生装置に割り当てることができる。また、前記鍵管理装置は、前記データ生成部で生成されたデータと、前記暗号文生成部で生成された暗号文と、前記選択鍵リスト生成部で生成されたリストとを記録媒体に記録する記録手段を更に備えることとしている。このような構成によって、不正に使用された再生装置では、再生することができないように記録媒体に暗号化したコンテンツを記録する鍵管理装置を得ることができる。また、前記鍵管理装置は、前記データ生成部で生成されたデータと、前記暗号文生成部で生成された暗号文と、前記選択鍵リスト生成部で生成されたリストとを複数の再生装置に送出する送出手段を更に備えることとしている。

【0081】このような構成によって、不正に使用された再生装置では、再生することができないようにした暗号化したコンテンツを送出する鍵管理装置を得ることができる。また、前記鍵管理情報記憶部は、前記鍵選択部により更新される鍵管理情報を記憶しておき、前記鍵記憶手段は、初期状態又はいずれかの更新時の状態に鍵管理情報を復帰させる復帰部を有することとを特徴とする請求項3記載の鍵管理装置。こととしている。

【0082】このような構成によって、過去のある時点

まで容易に鍵管理情報を復帰させることができる。また、前記無効とする鍵群の数の最大値を $2K$ とすると、前記鍵記憶手段に記憶されている木構造の数 L は $2K+1$ とすることとしている。このような構成によって、各再生装置の有する鍵群の鍵数や、鍵管理装置が記憶する鍵数、及び生成する暗号文の数等を最適とする木構造の数を得ることができる。

【0083】また、 N (N は、2以上の自然数)層の木構造の各ノードに配置された鍵の第 N 層の鍵から最上層の鍵に辿る異なる経路上の1つの鍵群を記憶している再生装置で再生される記録媒体であって、コンテンツをコンテンツ鍵で暗号化したデータを記憶しているデータ領域と、前記コンテンツ鍵を暗号化した少なくとも1つ以上の暗号文を記憶している暗号文領域と、前記暗号化に用いた鍵を識別する情報が記憶されている選択鍵リスト領域とを有し、暗号化に用いた選択鍵は、特定の再生装置以外の他の再生装置に記憶されている鍵群に含まれる1つの鍵と一致していることを特徴とする記録媒体。こととしている。

【0084】このような構成によって、記録媒体に記録されたデータは、不正に使用された再生装置以外の他の再生装置で再生することができる。また、本発明は、暗号化したデータを復号して再生する再生装置であって、各鍵は、 N (N は、2以上の自然数)層の木構造の各ノードに配置された鍵の木構造の第 N 層の鍵から最上層の鍵に辿る異なる経路上の1つの経路上にある鍵である N 個の鍵を記憶している鍵群記憶手段と、コンテンツをコンテンツ鍵で暗号化したデータと、前記コンテンツ鍵を暗号化した暗号文と、暗号化に用いた鍵を識別する情報とを取得する、暗号文は少なくとも1つ以上ある再生情報取得手段と、前記鍵を識別する情報で識別される鍵を前記鍵群記憶手段に記憶されている鍵から選択し、当該選択した鍵で対応する暗号文を復号してコンテンツ鍵を得るコンテンツ鍵復号手段と、前記データをコンテンツ鍵で復号して、コンテンツを再生するコンテンツ再生手段とを備えることとしている。

【0085】このような構成によって、取得したデータを自身の記憶するいずれかの鍵を用いて再生することのできる再生装置を得ることができる。また、前記再生装置は、録媒体に記録されたコンテンツをコンテンツ鍵で暗号化したデータと、前記コンテンツ鍵を暗号化した暗号文と、暗号化に用いた鍵を識別する情報とを読み出し、前記再生情報取得手段に与える読出手段を更に備えることとしている。

【0086】このような構成によって、記録媒体に記録されたデータを正当な再生装置で復号して再生することができる。また、前記再生装置は、鍵管理装置から送出されるコンテンツをコンテンツ鍵で暗号化したデータと、前記コンテンツ鍵を暗号化した暗号文と、暗号化に用いた鍵を識別する情報とを受信し、前記再生情報取得

手段に与える受信手段を更に備えることとしている。

【0087】このような構成によって、放送されるデータを正当な再生装置で受信して、復号して再生することができる。また、本発明の第1の目的は暗号化されたデータを復号して再生する複数の再生装置に割り当てた鍵を管理する鍵管理装置の鍵管理方法であって、木構造は少なくとも1つあり、木構造の第 N 層の鍵から最上層の鍵に辿る異なる経路上の鍵群は、それぞれ異なる再生装置に割り当てられており、 N (N は、2以上の自然数)層の木構造の各ノードに配置された鍵を鍵管理装置の記憶領域に記憶しており、前記各鍵群のうち、1つの再生装置が有する鍵群の情報の通知を受け付ける受付ステップと、当該鍵群の各鍵を無効鍵とし、無効鍵を経路上のノードに持つ他の再生装置に割り当てられた鍵群のうちから、前記無効鍵より一層下層の無効鍵でない鍵を選択する鍵選択ステップと、前記データの暗号化に用いたコンテンツ鍵を当該選択した鍵で暗号化した暗号文と、当該選択した鍵を特定する特定情報とからなる暗号情報を生成する暗号情報生成ステップとを有し、前記各再生装置は、割り当てられた N 個の鍵を記憶しており、前記特定情報により特定される鍵を用いて対応する暗号文を復号してコンテンツ鍵を得、前記データをそのコンテンツ鍵で復号して、コンテンツを再生することとしている。

【0088】このような方法によって、或る再生装置が有する鍵群を無効としたときに、他の再生装置では、1つの暗号文を自身の有するいずれかの鍵で復号してコンテンツ鍵を得ることができる。また、本発明の第1の目的は、暗号化されたデータを復号して再生する複数の再生装置に割り当てた鍵をコンピュータで管理する鍵管理プログラムであって、木構造は少なくとも1つあり、木構造の第 N 層の鍵から最上層の鍵に辿る異なる経路上の鍵群は、それぞれ異なる再生装置に割り当てられており、 N (N は、2以上の自然数)層の木構造の各ノードに配置された鍵を記憶領域に記憶しており、前記各鍵群のうち、1つの再生装置が有する鍵群の情報の通知を受け付ける受付ステップと、当該鍵群の各鍵を無効鍵とし、無効鍵を経路上のノードに持つ他の再生装置に割り当てられた鍵群のうちから、前記無効鍵より一層下層の無効鍵でない鍵を選択する鍵選択ステップと、前記データの暗号化に用いたコンテンツ鍵を当該選択した鍵で暗号化した暗号文と、当該選択した鍵を特定する特定情報とからなる暗号情報を生成する暗号情報生成ステップとを有し、前記各再生装置は、割り当てられた N 個の鍵を記憶しており、前記特定情報により特定される鍵を用いて対応する暗号文を復号してコンテンツ鍵を得、前記データをそのコンテンツ鍵で復号して、コンテンツを再生することとしている。

【0089】このようなプログラムを用いて、再生装置に割り当てた鍵を管理することができる。また、本発明の目的は、暗号化されたデータを復号して再生する複数の

の再生装置に割り当てた鍵を管理する鍵管理装置に適用されるコンピュータ読み取り可能な記録媒体は、木構造は少なくとも1つあり、木構造の第N層の鍵から最上層の鍵に辿る異なる経路上の鍵群は、それぞれ異なる再生装置に割り当てられており、N（Nは、2以上の自然数）層の木構造の各ノードに配置された鍵を記憶領域に記憶しており、前記各鍵群のうち、1つの再生装置が有する鍵群の情報の通知を受け付ける受付ステップと、当該鍵群の各鍵を無効鍵とし、無効鍵を経路上のノードに持つ他の再生装置に割り当てられた鍵群のうちから、前記無効鍵より一層下層の無効鍵でない鍵を選択する鍵選択ステップと、前記データの暗号化に用いたコンテンツ鍵を当該選択した鍵で暗号化した暗号文と、当該選択した鍵を特定する特定情報とからなる暗号情報を生成する暗号情報生成ステップとをコンピュータに実行させるプログラムを記録し、前記各再生装置は、割り当てられたN個の鍵を記憶しており、前記特定情報により特定される鍵を用いて対応する暗号文を復号してコンテンツ鍵を得、前記データをそのコンテンツ鍵で復号して、コンテンツを再生することとしている。

【0090】このような記録媒体を鍵管理装置に適用できる。また、本発明の第1の目的は、書き換え可能な記録媒体に暗号化したデータを記録する複数の記録装置と、記録媒体に記録された暗号化されたデータを復号して再生する複数の再生装置と、前記記録装置と前記再生装置とに割り当てた鍵を管理する鍵管理装置とからなるシステムであって、前記鍵管理装置は、木構造は少なくとも1つあり、木構造の第N層の鍵から最上層の鍵に辿る異なる経路上の鍵群は、それぞれ異なる記録装置と再生装置とに割り当てられているN（Nは、2以上の自然数）層の木構造の各ノードに配置された鍵を記憶している鍵記憶手段と、前記各鍵群のうち、1つの記録装置及び／又は再生装置が有する鍵群の情報の通知を受けると、当該鍵群の各鍵を無効鍵とし、無効鍵を経路上のノードに持つ他の記録装置及び／又は再生装置に割り当てられた鍵群のうちから、前記無効鍵より一層下層の無効鍵でない鍵を選択し、前記データの暗号化に用いたコンテンツ鍵を当該選択した鍵で暗号化した暗号文と、当該選択した鍵を特定する特定情報とからなる暗号情報を生成する暗号情報生成手段と、前記記録媒体に生成された暗号情報を記録する暗号情報記録手段とを備え、前記記録装置は、各鍵は、N（Nは、2以上の自然数）層の木構造の各ノードに配置された鍵の木構造の第N層の鍵から最上層の鍵に辿る異なる経路上の1つの経路上にある鍵であるN個の鍵を記憶している鍵群記憶手段と、前記記録媒体から暗号情報を読み出し、暗号文を特定情報で特定される鍵記憶手段に記憶されている鍵データで復号してコンテンツ鍵を得るコンテンツ鍵復号手段と、取得したコンテンツを得られたコンテンツ鍵で暗号化したデータを前記記録媒体に記録するコンテンツ暗号化手段と

を備え、前記再生装置は、各鍵は、N（Nは、2以上の自然数）層の木構造の各ノードに配置された鍵の木構造の第N層の鍵から最上層の鍵に辿る異なる経路上の1つの経路上にある鍵であるN個の鍵を記憶している鍵群記憶手段と、コンテンツをコンテンツ鍵で暗号化したデータと、前記コンテンツ鍵を暗号化した少なくとも1つ以上の暗号文と、暗号化に用いた鍵を特定する特定情報とを取得する再生情報取得手段と、前記特定情報で特定される鍵を前記鍵群記憶手段に記憶されている鍵から選択し、当該選択した鍵で対応する暗号文を復号してコンテンツ鍵を得るコンテンツ鍵復号手段と、前記データをコンテンツ鍵で復号して、コンテンツを再生するコンテンツ再生手段とを備えることとしている。

【0091】このような構成によって、正規な記録装置と再生装置とによってのみ、取得したコンテンツをコンテンツ鍵で暗号化したデータを記録媒体に記録することができ、記録媒体に記録された暗号化されたデータをコンテンツ鍵で復号してコンテンツを再生することができる。また、N（Nは、2以上の自然数）層の木構造の各ノードに配置された鍵の第N層の鍵から最上層の鍵に辿る異なる経路上の1つの鍵群を記憶している記録装置で、コンテンツをコンテンツ鍵で暗号化したデータが記録され、同様の他の1つの鍵群を記憶している再生装置で読み出されて暗号化されたデータがコンテンツ鍵で復号される書き換え可能な記録媒体であって、前記コンテンツ鍵を暗号化した暗号文を記憶している暗号文領域と、前記暗号化に用いた鍵を特定する情報が記憶されている選択鍵リスト領域と、前記記録装置で記録されるデータのための領域であるデータ領域とを有し、前記暗号文は少なくとも1つ以上あり、暗号化に用いた選択鍵は前記記録装置及び前記再生装置に記憶されている鍵群に含まれる1つの鍵と一致しており、前記データは、前記暗号文を前記鍵を特定する情報で特定された前記再生装置に記憶された選択鍵を用いて復号化されたコンテンツ鍵で復号されることとしている。

【0092】このような記録媒体は、正規な記録装置と正規な再生装置とによってのみ、コンテンツの記録と再生とが可能となる。また、書き換え可能な記録媒体に暗号化したデータを記録する複数の記録装置と、記録媒体に記録された暗号化されたデータを復号して再生する複数の再生装置とに割り当てた鍵を管理する鍵管理装置であって、木構造は少なくとも1つあり、木構造の第N層の鍵から最上層の鍵に辿る異なる経路上の鍵群は、それぞれ異なる記録装置と再生装置とに割り当てられているN（Nは、2以上の自然数）層の木構造の各ノードに配置された鍵を記憶している鍵記憶手段と、前記各鍵群のうち、1つの記録装置及び／又は再生装置が有する鍵群の情報の通知を受けると、当該鍵群の各鍵を無効鍵とし、無効鍵を経路上のノードに持つ他の記録装置及び／又は再生装置に割り当てられた鍵群のうちから、前記無効鍵

より一層下層の無効鍵でない鍵を選択し、前記データの暗号化に用いたコンテンツ鍵を当該選択した鍵で暗号化した暗号文と、当該選択した鍵を特定する特定情報とからなる暗号情報を生成する暗号情報生成手段と、前記記録媒体に生成された暗号情報を記録する暗号情報記録手段とを備えることとしている。

【0093】このような構成によって、記録装置と再生装置とに割り当てた鍵群を管理することができる。また、書き換え可能な記録媒体に暗号化したデータを記録する記録装置であって、各鍵は、N（Nは、2以上の自然数）層の木構造の各ノードに配置された鍵の木構造の第N層の鍵から最上層の鍵に辿る異なる経路上の1つの経路上にある鍵であるN個の鍵を記憶している鍵群記憶手段と、前記記録媒体から暗号情報を読み出し、暗号文を特定情報で特定される鍵群記憶手段に記憶されている鍵データで復号してコンテンツ鍵を得るコンテンツ鍵復号手段と、取得したコンテンツを得られたコンテンツ鍵で暗号化したデータを前記記録媒体に記録するコンテンツ暗号化手段とを備え、前記記録媒体には、前記データの暗号化に用いるコンテンツ鍵を当該選択した鍵で暗号化した暗号文と、当該選択した鍵を特定する特定情報とからなる暗号情報が記憶されていることとしている。

【0094】このような構成によって、正規な記録装置によってのみ、記録媒体にコンテンツをコンテンツ鍵で暗号化したデータを記録することができる。

【図面の簡単な説明】

【図1】本発明に係る鍵管理装置及び再生装置の実施の形態1の構成図である。

【図2】上記実施の形態の鍵管理情報記録部に記憶されている鍵管理情報の一例を木構造モデルで示した図である。

【図3】上記実施の形態の鍵管理情報記憶部に記憶され*

＊ている鍵管理情報の一例を示す図である。

【図4】上記実施の形態の鍵管理情報記憶部に記憶されている鍵管理情報の更新された状態の一例を示す図である。

【図5】上記実施の形態の記録部で記録媒体に記録される内容の一例を示す図である。

【図6】図4に示した更新された鍵管理情報に従い、記録媒体に記録される内容の一例を示す図である。

【図7】上記実施の形態の再生装置の鍵記憶部に記憶されている鍵情報の一例を示す図である。

【図8】上記実施の形態の鍵管理情報の更新処理の動作を説明するフローチャートである。

【図9】本発明に係る鍵管理装置の実施の形態2の鍵管理情報記憶部に記憶されている鍵管理情報の一例の木構造モデルを示した図である。

【図10】上記実施の形態の鍵管理情報記憶部に記憶されている鍵管理情報の一例を示す図である。

【図11】木構造の数の相違による鍵管理情報に基づく諸データの比較表の一例を示す図である。

【図12】本発明に係る鍵管理装置及び再生装置の実施の形態3の構成図である。

【図13】上記実施の形態の鍵管理装置で、一旦無効化された鍵を再度利用できるように復帰する動作を説明するフローチャートである。

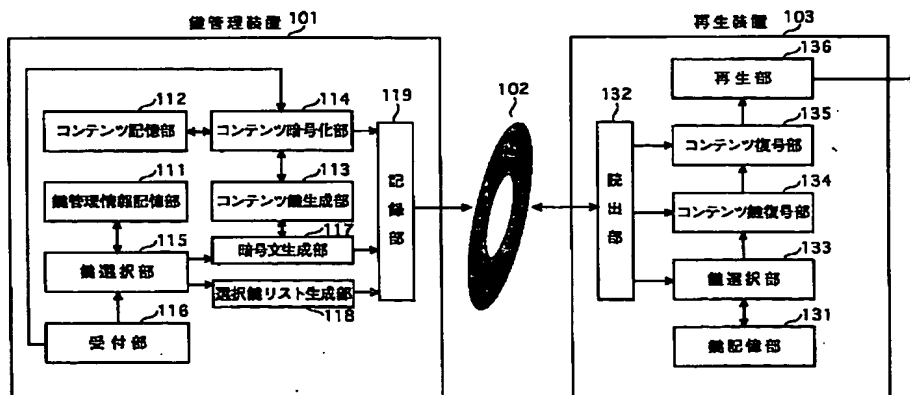
【図14】上記実施の形態で、新たに再生装置に鍵群を追加して割り当てる様子を説明する図である。

【図15】本発明に係る鍵管理システムの実施の形態4の概略を示す構成図である。

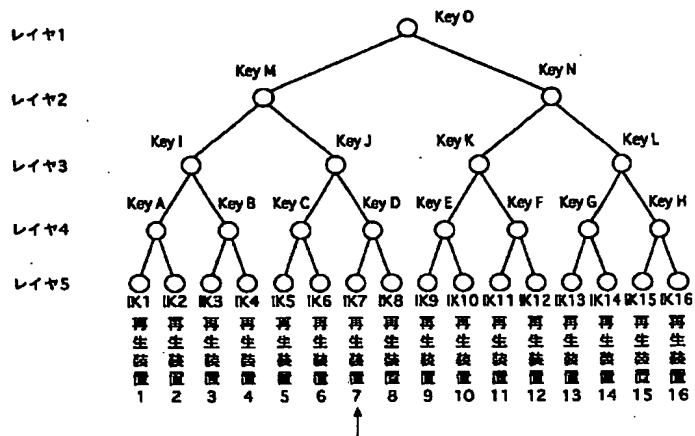
【図16】上記実施の形態の記録装置の構成図である。

【図17】上記実施の形態の再生装置の概略構成図である。

【図1】



【図2】



【図7】

鍵情報 701	
702 鍵 ID	703 鍵 データ
IK 1
Key A
Key I
Key M
Key O

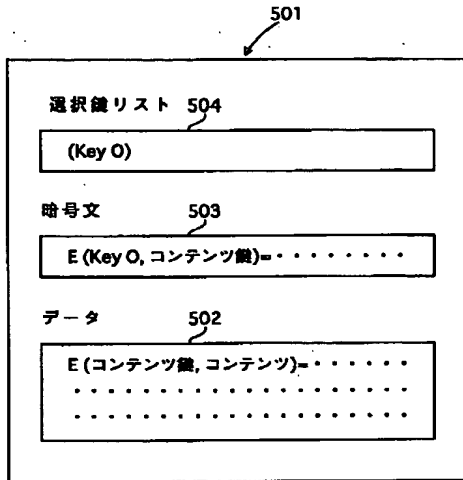
【図3】

鍵管理情報 301			
302 鍵 ID	303 鍵 データ	304 親鍵のID	305 鍵状態
Key O	11...11	1
Key M	Key O	0
Key N	Key O	0
Key I	Key M	0
Key J	Key M	0
Key K	Key N	0
⋮	⋮	⋮	⋮
Key A	Key I	0
Key B	Key I	0
Key C	Key J	0
Key D	Key J	0
⋮	⋮	⋮	⋮
IK 1	Key A	0
⋮	⋮	⋮	⋮
IK 7	Key D	0
IK 8	Key D	0
⋮	⋮	⋮	⋮
IK 16	Key H	0

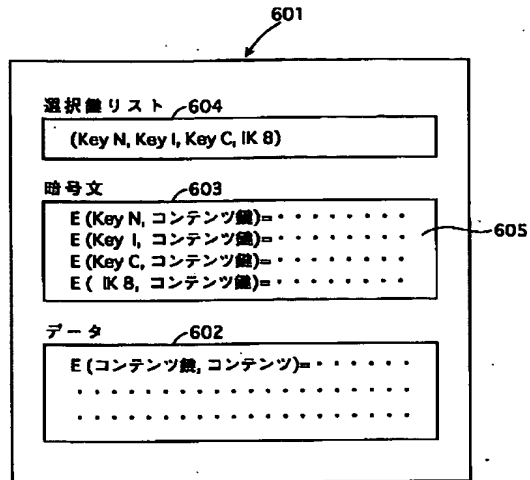
【図4】

鍵管理情報 401			
302 鍵 ID	303 鍵 データ	304 親鍵のID	305 鍵状態
Key O	11...11	-1
Key M	Key O	-1
Key N	Key O	1
Key I	Key M	1
Key J	Key M	-1
Key K	Key N	0
⋮	⋮	⋮	⋮
Key A	Key I	0
Key B	Key I	0
Key C	Key J	1
Key D	Key J	-1
⋮	⋮	⋮	⋮
IK 1	Key A	0
⋮	⋮	⋮	⋮
IK 7	Key D	-1
IK 8	Key D	1
⋮	⋮	⋮	⋮
IK 16	Key H	0

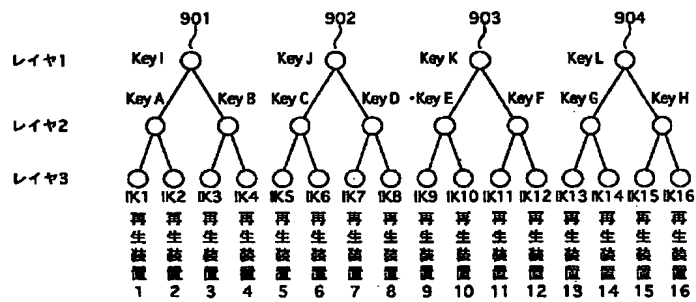
【図5】



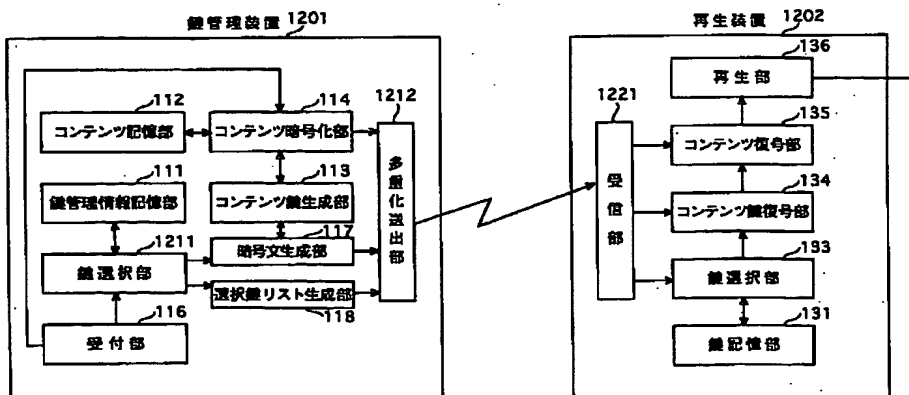
【図6】



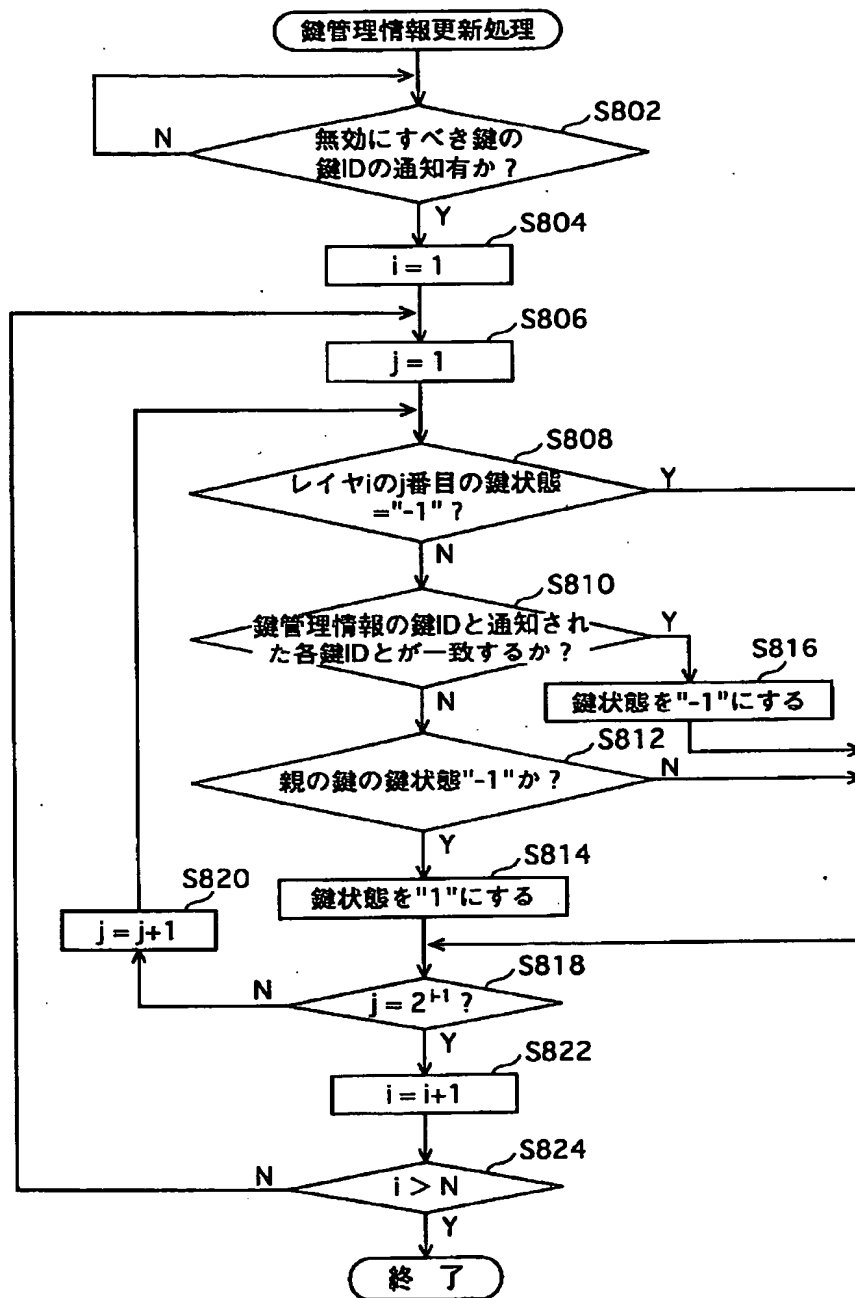
【図9】



【図12】



【図8】



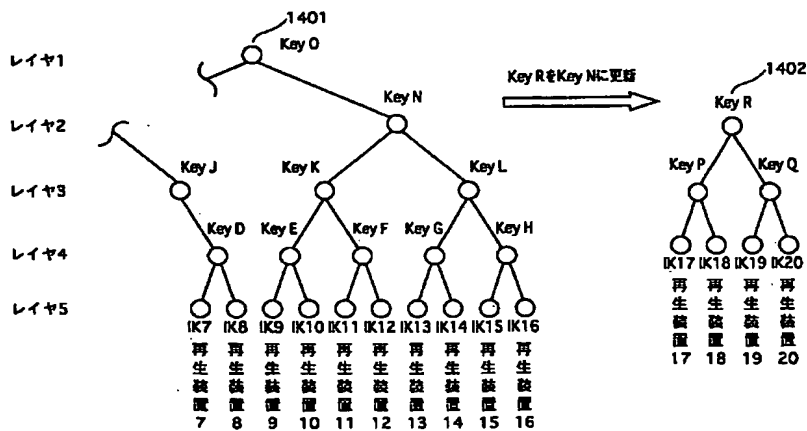
【図10】

鍵管理情報 1001			
1002	1003	1004	1005
鍵 ID	鍵 データ	組織のID	鍵状態
Key I	11...11	1
Key A	Key I	0
Key B	Key I	0
IK 1	Key A	0
IK 2	Key A	0
IK 3	Key B	0
IK 4	Key B	0
Key J	11...11	1
Key C	Key J	0
Key D	Key J	0
IK 5	Key C	0
IK 6	Key C	0
IK 7	Key D	0
IK 8	Key D	0
Key K	11...11	1
Key E	Key K	0
⋮	⋮	⋮	⋮
IK 12	Key F	0
Key L	11...11	1
⋮	⋮	⋮	⋮
IK 16	Key H	0

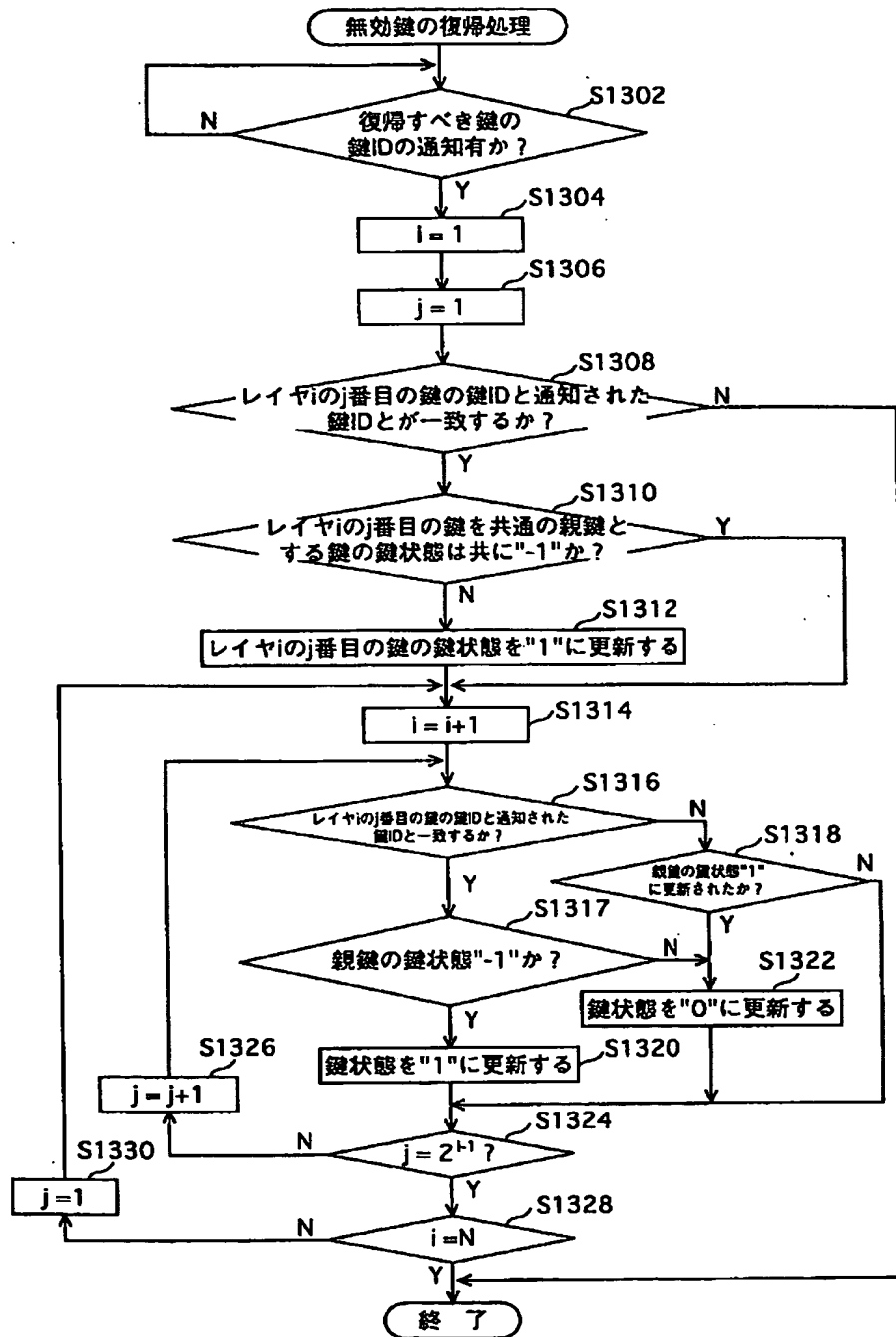
【図11】

比較表 1101				
1102	1103	1104	1105	1106
木構造の数	鍵数	不正使用された再生装置数	選択鍵数 = 暗号文数	再生装置での 鍵数
1	31	0	1	5
		1	4	
		2	6	
2	30	0	2	4
		1	4	
		2	6	
4	28	0	4	3
		1	5	
		2	6	
8	24	0	8	2
		1	8	
		2	8	

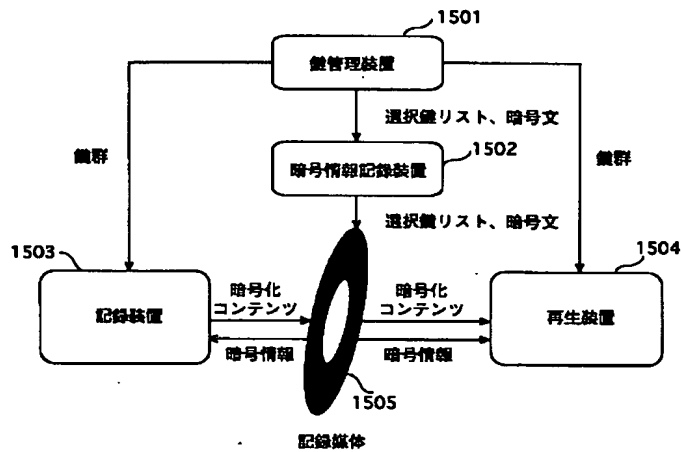
【図14】



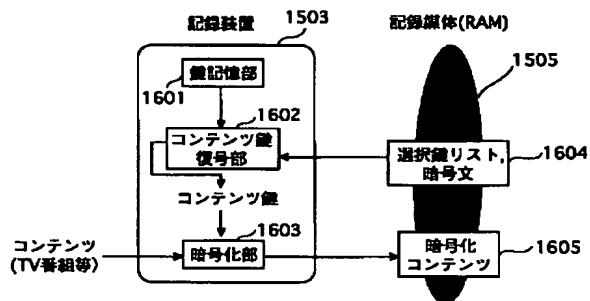
【図13】



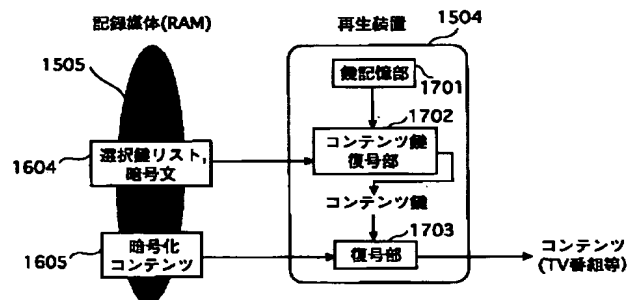
【図15】



【図16】



【図17】



フロントページの続き

(72)発明者 館林 誠
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

Fターム(参考) 5B017 AA03 BA07 CA05 CA16
5J104 AA34 EA06 EA07